(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001184264 A**

(43) Date of publication of application: **06.07.01**

(51) Int. Cl **G06F 12/14**
G06F 12/00

(21) Application number: **11358178**

(22) Date of filing: **16.12.99**

(71) Applicant: **INTERNATL BUSINESS MACH CORP <IBM>**

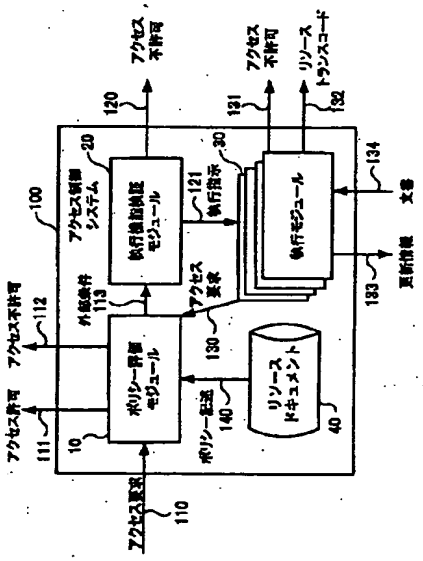
(72) Inventor: **NUMAO MASAYUKI**
KUDO MICHIYA
AMANO TOMIO

(54) **ACCESS CONTROL SYSTEM, ACCESS CONTROL METHOD, STORAGE MEDIUM, AND PROGRAM TRANSMITTING DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To make the permission of a conditional access possible to be evaluated in access control.

SOLUTION: This access control system 100 is provided with a resource document 40 for storing policy description, a policy evaluating module 10 for accepting an access request 110 for performing access from the outside part to a data file and for extracting and evaluating policy description related with data to be accessed of the access request 110 from the resource document 40 and for deciding whether or not the access request 110 should be permitted, an executing function verifying module 20 for judging whether or not the evaluation or realization of a condition which can not be evaluated only from the information of the policy evaluating module 10 is possible when the condition is present in the extracted policy description, and an executing module 30 for executing the evaluation or realization of the condition whose evaluation or execution is determined as possible by the executing function verifying module 20.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－184264
（P2001－184264A）
(43)公開日　平成13年７月６日(2001.7.6)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
G06F	12/14	320	G06F	12/14	320A	5B017
	12/00	537		12/00	537A	5B082

審査請求　有　　請求項の数19　ＯＬ　（全 19 頁）

(21)出願番号　特願平11－358178

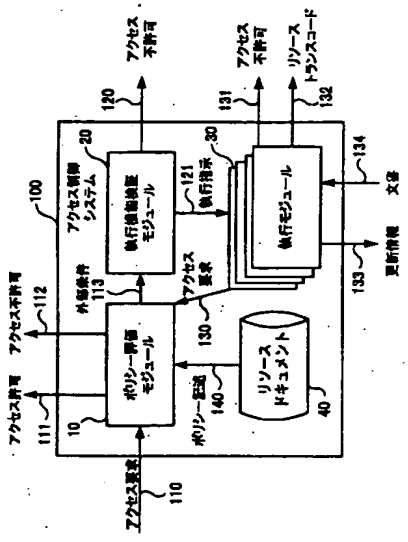
(22)出願日　平成11年12月16日(1999.12.16)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(74)代理人　100086243
弁理士　坂口　博　（外３名）

最終頁に続く

(54)【発明の名称】　アクセス制御システム、アクセス制御方法、記憶媒体、及びプログラム伝送装置

(57)【要約】
【課題】　アクセス制御において、条件付きのアクセス許可を評価できるようにする。
【解決手段】　アクセス制御システム１００であって、ポリシー記述を格納したリソースドキュメント４０と、外部からデータファイルにアクセスするためのアクセス要求１１０を受け付けて、リソースドキュメント４０からこのアクセス要求１１０のアクセス対象であるデータに関連付けられたポリシー記述を取り出して評価することにより、このアクセス要求１１０を許可するか否かを決定するポリシー評価モジュール１０と、取り出されたこのポリシー記述中に、ポリシー評価モジュール１０が持つ情報だけでは評価できない条件がある場合に、この条件の評価または実現が可能かどうかを判断する執行機能検証モジュール２０と、この執行機能検証モジュール２０により評価または実現が可能であると判断された条件の評価または実現を実行する執行モジュール３０とを備える。



1

【特許請求の範囲】

【請求項１】　データファイルに格納されているデータに関連するポリシー記述を格納したリソースドキュメントと、

外部から前記データファイルにアクセスするためのアクセス要求を受け付けて、前記リソースドキュメントから当該アクセス要求のアクセス対象であるデータに関連付けられたポリシー記述を取り出して評価することにより、当該アクセス要求を許可するか否かを決定するポリシー評価手段と、

取り出された前記ポリシー記述中に、前記ポリシー評価手段が持つ情報だけでは評価できない条件がある場合に、当該条件の評価または実現が可能かどうかを判断する執行機能検証手段と、

前記執行機能検証手段により評価または実現が可能であると判断された前記条件の評価または実現を実行する執行手段とを備えることを特徴とするアクセス制御システム。

【請求項２】　前記執行手段は、前記ポリシー評価手段が持つ情報だけでは評価できない条件に対する評価または実現の内容に応じて複数設けることができ、

前記執行機能検証手段は、前記執行手段が複数ある場合に、いずれの前記執行手段が前記ポリシー評価手段から受け取った前記条件の評価または実現を可能かについてさらに検証することを特徴とする請求項１に記載のアクセス制御システム。

【請求項３】　前記執行手段は、前記執行機能検証手段により評価または実現が可能であると判断された前記条件に対する評価または実現を実行するために他のデータ部分に対するアクセスを要する場合に、前記ポリシー評価手段に対して当該データ部分へのアクセス要求を発行し、

前記ポリシー評価手段は、外部から受け付けるアクセス要求と同様に、前記執行手段からなされたアクセス要求に対しても、アクセス対象であるデータに関連付けられたポリシー記述の評価を行うことを特徴とする請求項１に記載のアクセス制御システム。

【請求項４】　前記執行手段は、

データファイル中の書き込みまたは変更を行う部分を検出して前記ポリシー評価手段にアクセス要求を発行する書き込み／変更対象検出手段と、

前記ポリシー評価手段から前記アクセス要求に対するアクセス許可の回答を受けた場合に、前記データ部分への書き込みまたは変更を実行する書き込み／変更実行手段とを備え、

前記書き込み／変更実行手段は、プラグインにより所望の機能を用意できることを特徴とする請求項３に記載のアクセス制御システム。

【請求項５】　外部から所定のデータファイルにアクセスするためのアクセス要求を受け付けて、アクセス対象であるデータに関連付けられたポリシー記述を評価することにより、当該アクセス要求を許可するか否かを決定するアクセス制御方法において、

アクセス要求を受け付けて、当該アクセス要求のアクセス対象であるデータに関連付けられたポリシー記述を取得するステップと、

取得された前記ポリシー記述中の条件を評価するステップと、

取得された前記ポリシー記述中にそのままでは評価できない条件がある場合に、当該条件を満足するための処理が執行可能かどうかを判断するステップと、

前記条件を満足するための処理が執行可能であると判断された場合に、当該処理を執行するステップと、

前記条件を満足するための処理が執行された後に、前記ポリシー記述中の全ての条件に対する評価結果に応じて、前記アクセス要求を許可するか否かを決定するステップとを含むことを特徴とするアクセス制御方法。

【請求項６】　前記ポリシー記述中の条件を評価するステップは、

前記受け付けたアクセス要求のパラメータと前記取得したポリシー記述中の規則とを照合して合致する規則を検出するステップと、

検出された前記規則の条件部を評価するステップと、

前記規則の条件部がそのままでは評価することができない場合に、当該条件を集めて、当該条件を満足するための処理が執行可能かどうかを判断するステップに移行するステップとを含むことを特徴とする請求項５に記載のアクセス制御方法。

【請求項７】　前記ポリシー記述中の規則の条件部を評価するステップに先だって、前記アクセス要求のパラメータと合致する前記規則が複数検出された場合に、所定の規則に基づいて前記規則に対する評価の優先順位を決定するステップを更に含むことを特徴とする請求項６に記載のアクセス制御方法。

【請求項８】　前記ポリシー記述中の条件を満足するための処理が執行可能かどうかを判断するステップは、

前記ポリシー記述中の条件を評価するステップにおいて作成された、前記ポリシー記述中の情報のみに基づいて評価することができない前記規則の条件の集合を受け付けて、個々の当該条件を取り出すステップと、

取り出された各条件ごとに前記条件を満足するための処理を執行する機能が用意されているかどうかを判定するステップと、

前記条件を満足するための処理を執行する機能が用意されていると判定した場合に、当該機能を呼び出すステップとを含むことを特徴とする請求項６に記載のアクセス制御方法。

【請求項９】　前記ポリシー記述中の条件を満足するための処理を執行するステップは、

前記ポリシー記述中の条件を満足するための処理が執行

可能かどうかを判断するステップにおいて呼び出された機能により、所定のデータファイル中から、前記ポリシー記述中の条件に基づいて書き込みまたは変更を行うデータ部分を検出するステップと、
前記書き込みまたは変更を行うために必要なアクセス要求を発行するステップと、
前記書き込みまたは変更を行うために必要な前記アクセス要求に対するアクセス許可の回答を受けた場合に、前記データ部分への書き込みまたは変更を実行するステップとを含むことを特徴とする請求項８に記載のアクセス制御方法。

【請求項１０】　コンピュータに実行させるプログラムを当該コンピュータの入力手段が読取可能に記憶した記憶媒体において、
前記プログラムは、
外部から所定のデータファイルにアクセスするためのアクセス要求を受け付けて、当該アクセス要求のアクセス対象であるデータに関連付けられたポリシー記述を取得する処理と、
取得された前記ポリシー記述中の条件を評価する処理と、
取得された前記ポリシー記述中にそのままでは評価できない条件がある場合に、当該条件を満足するための処理が執行可能かどうかを判断する処理と、
前記条件を満足するための処理が執行可能であると判断された場合に、当該処理を執行する処理と、
前記条件を満足するための処理が執行された後に、前記ポリシー記述中の全ての条件に対する評価結果に応じて、前記アクセス要求を許可するか否かを決定する処理とを前記コンピュータに実行させることを特徴とする記憶媒体。

【請求項１１】　前記プログラムは、前記ポリシー記述中の条件を満足するための処理を執行するために、
前記ポリシー記述中の条件を満足するための処理が執行可能かどうかを判断する処理において呼び出された機能により、所定のデータファイル中から、前記ポリシー記述中の条件に基づいて書き込みまたは変更を行うデータ部分を検出する処理と、
前記書き込みまたは変更を行うために必要なアクセス要求を発行する処理と、
前記書き込みまたは変更を行うために必要な前記アクセス要求に対するアクセス許可の回答を受けた場合に、前記データ部分への書き込みまたは変更を実行する処理とを前記コンピュータに実行させることを特徴とする請求項１０に記載の記憶媒体。

【請求項１２】　コンピュータに、
外部から所定のデータファイルにアクセスするためのアクセス要求を受け付けて、当該アクセス要求のアクセス対象であるデータに関連付けられたポリシー記述を取得する処理と、取得された前記ポリシー記述中の条件を評価する処理と、取得された前記ポリシー記述中にそのままでは評価できない条件がある場合に、当該条件を満足するための処理が執行可能かどうかを判断する処理と、
前記条件を満足するための処理が執行可能であると判断された場合に、当該処理を執行する処理と、前記条件を満足するための処理が執行された後に、前記ポリシー記述中の全ての条件に対する評価結果に応じて、前記アクセス要求を許可するか否かを決定する処理とを実行させるプログラムを記憶する記憶手段と、
前記記憶手段から前記プログラムを読み出して当該プログラムを送信する送信手段とを備えたことを特徴とするプログラム伝送装置。

【請求項１３】　前記記憶手段に記憶されているプログラムは、前記ポリシー記述中の条件を満足するための処理を執行するために、
前記ポリシー記述中の条件を満足するための処理が執行可能かどうかを判断する処理において呼び出された機能により、所定のデータファイル中から、前記ポリシー記述中の条件に基づいて書き込みまたは変更を行うデータ部分を検出する処理と、
前記書き込みまたは変更を行うために必要なアクセス要求を発行する処理と、
前記書き込みまたは変更を行うために必要な前記アクセス要求に対するアクセス許可の回答を受けた場合に、前記データ部分への書き込みまたは変更を実行する処理とをコンピュータに実行させることを特徴とする請求項１２に記載のプログラム伝送装置。

【請求項１４】　単一のソースで記述された情報に関してフォーマットの変換が可能ならば読み取りを許可するという条件を持つポリシー記述を格納する手段と、
前記ポリシー記述に合致する所定のアクセス要求を受け付けた場合に、前記条件を満足するための、フォーマットを変換する処理を行う機能があるかどうかを調べると共に、当該機能があると判断した場合に、当該機能を呼び出して前記条件を満足するための処理を実行させる手段と、
前記条件を満足するための処理が実行された場合に、前記アクセス要求に対してアクセスを許可する手段とを備えることを特徴とするアクセス制御システム。

【請求項１５】　アクセス対象である文書に電子透かしを埋め込むならば読みとりを許可するという条件を持つポリシー記述を格納する手段と、
前記ポリシー記述に合致する所定のアクセス要求を受け付けた場合に、前記条件を満足するための、文書に電子透かしを埋め込む処理を行う機能があるかどうかを調べると共に、当該機能があると判断した場合に、当該機能を呼び出して前記条件を満足するための処理を実行させる手段と、
前記条件を満足するための処理が実行された場合に、前記アクセス要求に対してアクセスを許可する手段とを備

えることを特徴とするアクセス制御システム。

【請求項１６】　アクセス対象である文書にアクセス履歴を書き込むならば当該文書へのアクセスを許可するという条件を持つポリシー記述を格納する手段と、
前記ポリシー記述に合致する所定のアクセス要求を受け付けた場合に、前記条件を満足するための、文書にアクセス履歴を書き込む処理を行う機能があるかどうかを調べると共に、当該機能があると判断した場合に、当該機能を呼び出して前記条件を満足するための処理を実行させる手段と、
前記条件を満足するための処理が実行された場合に、前記アクセス要求に対してアクセスを許可する手段とを備えることを特徴とするアクセス制御システム。

【請求項１７】　前記アクセス対象である文書にアクセス履歴を書き込む機能において、当該アクセス履歴の書き込みを行うための前記文書へのアクセス要求を再帰的に行う手段を更に備えることを特徴とする請求項１６に記載のアクセス制御システム。

【請求項１８】　アクセス対象である文書に対してアクセス時のタイムスタンプをアクセス履歴として書き込むならばアクセスを許可するという条件を持つポリシー記述を格納する手段と、
前記ポリシー記述に合致する所定のアクセス要求を受け付けた場合に、前記条件を満足するための、文書にアクセス時のタイムスタンプをアクセス履歴として書き込む処理を行う機能があるかどうかを調べると共に、当該機能があると判断した場合に、当該機能を呼び出して前記条件を満足するための処理を実行させる手段と、
前記条件を満足するための処理が実行された場合に、前記アクセス要求に対してアクセスを許可する手段とを備えることを特徴とするアクセス制御システム。

【請求項１９】　データファイルに格納されているデータに関連するポリシー記述を格納したリソースドキュメントと、
外部から前記データファイルにアクセスするためのアクセス要求を受け付けて、前記リソースドキュメントから当該アクセス要求のアクセス対象であるデータに関連付けられたポリシー記述を取り出して評価することにより、当該アクセス要求を許可するか否かを決定するポリシー評価手段と、
取り出された前記ポリシー記述中に、前記ポリシー評価手段が持つ情報だけでは評価できない条件がある場合に、他の処理を行うことにより当該条件の評価または実現が可能かどうかを判断する執行機能検証手段とを備えることを特徴とするアクセス制御システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、アクセス制御におけるポリシー記述に対する評価とこれを実現するための条件部の執行とを行う方法に関する。

【０００２】

【従来の技術】従来、データファイルへのアクセス制御におけるポリシーの記述手段としては、ＡＴＴのKeyNotes〔BFIK99〕(PolicyMaker〔BRL96〕)、GACL〔WL93〕〔WL98〕、ASL〔JSSB97〕などが知られている。アクセスの可否を判定するためのルールである、これらのポリシー記述は、いずれもアクセス・コントロール・リスト（ＡＣＬ）と呼ばれる（Subj，Obj，Op）の３つ組リストを基本にしている。これは、アクセスの主体（Subj）がアクセスの対象（Obj）に対して、ある操作（Op）が許されることを示している。したがって、全てのアクセス要求に答えるためには、あらゆる３つ組みの組み合わせに対してＡＣＬを用意する必要がある。

【０００３】上記のポリシー記述手段では、これを簡略化するために、変数を使ったパターンマッチングを記述できるようにし、さらに、変数を限定する条件式を書くために、ACL(Subj，Obj，Op)≦Cond(Subj，Obj，Op)というようなルールを導入している。すなわち、アクセス要求におけるあらゆる３つ組みに対応するＡＣＬを用意するのは大がかりであるし困難であるので、変数を用いてポリシーを抽象化しておき、その変数に該当するアクセス要求については対応するＡＣＬにしたがってアクセス制御を行う。

【０００４】また、ＡＣＬにおける制御対象の操作の記述方法には２種類ある。すなわち、許される操作だけを記述するものと、許される操作と許されない操作の両方を記述できるものである。前者は閉世界仮説（Closed World Assumption）とともに用いられる。閉世界仮説では、あるアクセス要求に対して、それに対応するＡＣＬがない場合にはその操作は許されないという解釈になる。したがって、ＡＣＬに許される操作だけを記述しておき、アクセス要求がＡＣＬのどのエントリにも合致しない場合は無条件に当該操作を拒絶する。一方、後者はGACLなどに用いられているが、明示的な負の操作が指定されていない限り、操作を許すといったDefault推論が用いられている。

【０００５】ポリシーの評価方法にこうした差異はあるものの、従来のポリシー評価システムは全て、ポリシーを評価した結果をＹｅｓまたはＮｏの２値で返すようにしている。つまり、質問文？-ACL（subj，obj，op）に対して１または０のいずれかの値が返る。

【０００６】

【発明が解決しようとする課題】上述したように、従来のアクセス制御におけるポリシーの評価技術は、アクセス要求に対してポリシーを評価した結果をＹｅｓまたはＮｏの２値のいずれかとしている。すなわち、アクセス要求に対してこれを許すか許さないかの判断しか行うことができない。このため、ある条件を満たせばＹｅｓ（Yes with condition）というような応答を行うことができず、柔軟性に欠けていた。

【０００７】このため、データの暗号化やフォーマット変換を行うならばアクセスを許すといった実施インストラクションを行ったり、読み出したデータに電子透かしを入れたり、アクセスログの書き込みを行ったり、時間条件に応じてアクセスを許したりするというように、様々な条件に基づく複雑なアクセス制御を汎用的に実施することができなかった。

【０００８】本発明は以上のような技術的課題を解決するためになされたものであって、アクセス制御において、アクセス要求に対してアクセスを許すか許さないかを判断するだけでなく、ある条件を満たせばアクセスを許すという条件付きのアクセス許可を評価できるようにすることを目的とする。

【０００９】更に、条件付きのアクセス許可において評価される条件が更に他の条件を満足することを要求する場合に、再帰的に当該他の条件に対する評価も行うことができるようにすることを他の目的とする。

【００１０】

【課題を解決するための手段】かかる目的のもと、本発明は、アクセス制御システムであって、データファイルに格納されているデータに関連するポリシー記述を格納したリソースドキュメントと、外部からデータファイルにアクセスするためのアクセス要求を受け付けて、リソースドキュメントからこのアクセス要求のアクセス対象であるデータに関連付けられたポリシー記述を取り出して評価することにより、このアクセス要求を許可するか否かを決定するポリシー評価手段と、取り出されたこのポリシー記述中に、ポリシー評価手段が持つ情報だけでは評価できない条件がある場合に、この条件の評価または実現が可能かどうかを判断する執行機能検証手段と、この執行機能検証手段により評価または実現が可能であると判断された条件の評価または実現を実行する執行手段とを備えることを特徴としている。

【００１１】ここで、執行手段は、ポリシー評価手段が持つ情報だけでは評価できない条件に対する評価または実現の内容に応じて複数設けることができ、執行機能検証手段は、執行手段が複数ある場合に、いずれの執行手段がポリシー評価手段から受け取った条件の評価または実現を可能かについてさらに検証することを特徴としている。これにより、条件の内容に柔軟に対応することが可能となる点で好ましい。また、条件の評価または実現が可能な執行手段の検証には、例えば、執行手段のコンポーネントとそのコンポーネントが執行できる条件とを関連付けて格納したリストを用いることができる。

【００１２】さらに執行手段は、執行機能検証手段により評価または実現が可能であると判断された条件に対する評価または実現を実行するために他のデータ部分に対するアクセスを要する場合に、ポリシー評価手段に対してこのデータ部分へのアクセス要求を発行し、ポリシー評価手段は、外部から受け付けるアクセス要求と同様に、執行手段からなされたアクセス要求に対しても、アクセス対象であるデータに関連付けられたポリシー記述の評価を行うことを特徴としている。これにより、条件の評価または実現のために再帰的にアクセス要求を行うことが可能となる点で優れている。尚、データ部分とは、アクセス対象である文書の他の部分であっても、他の文書の所定の部分であっても良い。

【００１３】この執行手段は、データファイル中の書き込みまたは変更を行う部分を検出してポリシー評価手段にアクセス要求を発行する書き込み／変更対象検出手段と、ポリシー評価手段からこのアクセス要求に対するアクセス許可の回答を受けた場合に、データ部分への書き込みまたは変更を実行する書き込み／変更実行手段とを備え、この書き込み／変更実行手段は、プラグインにより所望の機能を用意できることを特徴としている。これにより、条件に対する評価または実現に複雑な処理を要する場合にも、プラグインで対応機能を追加できるため、柔軟に対応することができる点で好ましい。書き込み／変更実行手段としては、例えば、アクセス対象がＸＭＬ文書である場合には、ＸＭＬデータと変換ルールを読み込んで新たなＸＭＬデータを生成する標準のツールであるＸＳＬプロセッサを用いることができる。この場合も、複雑な処理を実現するためにプラグインソフトを追加できるのは同様である。

【００１４】また、本発明は、外部から所定のデータファイルにアクセスするためのアクセス要求を受け付けて、アクセス対象であるデータに関連付けられたポリシー記述を評価することにより、このアクセス要求を許可するか否かを決定するアクセス制御方法において、アクセス要求を受け付けて、アクセス要求のアクセス対象であるデータに関連付けられたポリシー記述を取得するステップと、取得されたポリシー記述中の条件を評価するステップと、取得されたポリシー記述中にそのままでは評価できない条件がある場合に、この条件を満足するための処理が執行可能かどうかを判断するステップと、この条件を満足するための処理が執行可能であると判断された場合に、かかる処理を執行するステップと、この条件を満足するための処理が執行された後に、ポリシー記述中の全ての条件に対する評価結果に応じて、このアクセス要求を許可するか否かを決定するステップとを含むことを特徴としている。なお、条件を満足するための処理とは、具体的にはかかる条件を評価または実現するための処理である。

【００１５】ここで、ポリシー記述中の条件を評価するステップは、受け付けたアクセス要求のパラメータと前記取得したポリシー記述中の規則とを照合して合致する規則を検出するステップと、検出された規則の条件部を評価するステップと、この規則の条件部がそのままでは評価することができない場合に、かかる条件を集めて、この条件を満足するための処理が執行可能かどうかを判

断するステップに移行するステップとを含むことを特徴としている。さらにここで、ポリシー記述中の規則の条件部を評価するステップに先だって、アクセス要求のパラメータと合致する規則が複数検出された場合に、所定の規則に基づいて前記規則に対する評価の優先順位を決定するステップを更に含むことを特徴としている。このようにすれば、条件に合致する規則が複数ある場合に適切な規則を適用することができる。尚、優先順位は、ポリシー規則に優先度を指定しておき、その優先度にしたがって決定するようにしても良い。また、同一の条件に合致する規則として、アクセス不許可となるポリシー規則とアクセス許可となるポリシー規則とがある場合は、不用意にアクセスを許可してしまうことを防止するため、アクセス不許可となるポリシー規則を優先させるようにしても良い。

【００１６】さらに、ポリシー記述中の条件を満足するための処理が執行可能かどうかを判断するステップは、ポリシー記述中の条件を評価するステップにおいて作成された、ポリシー記述中の情報のみに基づいて評価することができない規則の条件の集合を受け付けて、個々の条件を取り出すステップと、取り出された各条件ごとにこの条件を満足するための処理を執行する機能が用意されているかどうかを判定するステップと、この条件を満足するための処理を執行する機能が用意されていると判定した場合に、この機能を呼び出すステップとを含むことを特徴としている。条件を満足するための処理を執行する機能が用意されているかどうかを検証するには、上述したように、執行手段のコンポーネントとそのコンポーネントが執行できる条件とを関連付けて格納したリストを用いることができる。

【００１７】さらに、ポリシー記述中の条件を満足するための処理を執行するステップは、このポリシー記述中の条件を満足するための処理が執行可能かどうかを判断するステップにおいて呼び出された機能により、所定のデータファイル中から、ポリシー記述中の条件に基づいて書き込みまたは変更を行うデータ部分を検出するステップと、書き込みまたは変更を行うために必要なアクセス要求を発行するステップと、この書き込みまたは変更を行うために必要なアクセス要求に対するアクセス許可の回答を受けた場合に、データ部分への書き込みまたは変更を実行するステップとを含むことを特徴としている。尚、データ部分とは、上述したように、アクセス対象である文書の他の部分であっても、他の文書の所定の部分であっても良い。

【００１８】また、本発明は、コンピュータに実行させるプログラムをこのコンピュータの入力手段が読取可能に記憶した記憶媒体において、このプログラムは、外部から所定のデータファイルにアクセスするためのアクセス要求を受け付けて、このアクセス要求のアクセス対象であるデータに関連付けられたポリシー記述を取得する処理と、取得されたポリシー記述中の条件を評価する処理と、取得されたポリシー記述中にそのままでは評価できない条件がある場合に、この条件を満足するための処理が執行可能かどうかを判断する処理と、この条件を満足するための処理が執行可能であると判断された場合に、かかる処理を執行する処理と、この条件を満足するための処理が執行された後に、ポリシー記述中の全ての条件に対する評価結果に応じて、このアクセス要求を許可するか否かを決定する処理とをコンピュータに実行させることを特徴としている。このようにすれば、このプログラムをロードしたコンピュータにおいて、条件付きのアクセス許可に対応するアクセス評価を実現することができる。

【００１９】ここで、プログラムは、ポリシー記述中の条件を満足するための処理を執行するために、ポリシー記述中の条件を満足するための処理が執行可能かどうかを判断する処理において呼び出された機能により、所定のデータファイル中から、ポリシー記述中の条件に基づいて書き込みまたは変更を行うデータ部分を検出する処理と、書き込みまたは変更を行うために必要なアクセス要求を発行する処理と、書き込みまたは変更を行うために必要なアクセス要求に対するアクセス許可の回答を受けた場合に、データ部分への書き込みまたは変更を実行する処理とを前記コンピュータに実行させることを特徴としている。このようにすれば、このプログラムをロードしたコンピュータにおいて、条件付きのアクセス許可に対し、かかる条件を満足するために再帰的にアクセス要求を行うことが可能となる。

【００２０】また、本発明は、コンピュータに、外部から所定のデータファイルにアクセスするためのアクセス要求を受け付けて、このアクセス要求のアクセス対象であるデータに関連付けられたポリシー記述を取得する処理と、取得されたポリシー記述中の条件を評価する処理と、取得されたポリシー記述中にそのままでは評価できない条件がある場合に、この条件を満足するための処理が執行可能かどうかを判断する処理と、この条件を満足するための処理が執行可能であると判断された場合に、かかる処理を執行する処理と、この条件を満足するための処理が執行された後に、ポリシー記述中の全ての条件に対する評価結果に応じて、このアクセス要求を許可するか否かを決定する処理とを実行させるプログラムを記憶する記憶手段と、この記憶手段からこのプログラムを読み出して送信する送信手段とを備えたことを特徴としている。このようなプログラム伝送装置により、プログラムの提供形態としてＣＤ－ＲＯＭ等の記憶媒体を介することなく、顧客に対して本発明の技術を提供することが可能となる。

【００２１】ここで、記憶手段に記憶されているプログラムは、ポリシー記述中の条件を満足するための処理を執行するために、ポリシー記述中の条件を満足するため

の処理が執行可能かどうかを判断する処理において呼び出された機能により、所定のデータファイル中から、ポリシー記述中の条件に基づいて書き込みまたは変更を行うデータ部分を検出する処理と、書き込みまたは変更を行うために必要なアクセス要求を発行する処理と、書き込みまたは変更を行うために必要なアクセス要求に対するアクセス許可の回答を受けた場合に、データ部分への書き込みまたは変更を実行する処理とをコンピュータに実行させることを特徴としている。

【００２２】また、本発明は、単一のソースで記述された情報に関してフォーマットの変換が可能ならば読み取りを許可するという条件を持つポリシー記述を格納する手段と、このポリシー記述に合致する所定のアクセス要求を受け付けた場合に、かかる条件を満足するための、フォーマットを変換する処理を行う機能があるかどうかを調べると共に、この機能があると判断した場合に、この機能を呼び出してかかる条件を満足するための処理を実行させる手段と、この条件を満足するための処理が実行された場合に、このアクセス要求に対してアクセスを許可する手段とを備えることを特徴としている。このようにすれば、トランスコーディングを条件としてアクセス許可を行うことが可能となる。

【００２３】また、本発明は、アクセス対象である文書に電子透かしを埋め込むならば読みとりを許可するという条件を持つポリシー記述を格納する手段と、このポリシー記述に合致する所定のアクセス要求を受け付けた場合に、かかる条件を満足するための、文書に電子透かしを埋め込む処理を行う機能があるかどうかを調べると共に、この機能があると判断した場合に、この機能を呼び出してかかる条件を満足するための処理を実行させる手段と、この条件を満足するための処理が実行された場合に、このアクセス要求に対してアクセスを許可する手段とを備えることを特徴としている。このようにすれば、トランスコーディングの一態様として、文書に電子透かしを埋め込むことを条件としてアクセス許可を行うことが可能となる。なお、トランスコーディングの更に別の態様として文書の暗号化についても同様に行うことが可能である。

【００２４】また、本発明は、アクセス対象である文書にアクセス履歴を書き込むならばこの文書へのアクセスを許可するという条件を持つポリシー記述を格納する手段と、このポリシー記述に合致する所定のアクセス要求を受け付けた場合に、かかる条件を満足するための、文書にアクセス履歴を書き込む処理を行う機能があるかどうかを調べると共に、この機能があると判断した場合に、この機能を呼び出してかかる条件を満足するための処理を実行させる手段と、この条件を満足するための処理が実行された場合に、このアクセス要求に対してアクセスを許可する手段とを備えることを特徴としている。このようにすれば、文書にアクセス履歴を残すことを条件としてアクセス許可を行うことが可能となる。ここで、アクセス対象である文書にアクセス履歴を書き込む機能において、このアクセス履歴の書き込みを行うための文書へのアクセス要求を再帰的に行う手段を更に備えることを特徴としている。このようにすれば、文書にアクセス履歴を書き込むためにこの文書に再帰的にアクセスすること自体をアクセス許可の評価対象として、セキュリティーを高めることができる。なお、アクセス履歴を書きこむ対象はアクセス対象となった文書でもまた別の文書の一部であってもよい。

【００２５】また、本発明は、アクセス対象である文書に対してアクセス時のタイムスタンプをアクセス履歴として書き込むならばアクセスを許可するという条件を持つポリシー記述を格納する手段と、このポリシー記述に合致する所定のアクセス要求を受け付けた場合に、かかる条件を満足するための、文書にアクセス時のタイムスタンプをアクセス履歴として書き込む処理を行う機能があるかどうかを調べると共に、この機能があると判断した場合に、この機能を呼び出してかかる条件を満足するための処理を実行させる手段と、この条件を満足するための処理が実行された場合に、このアクセス要求に対してアクセスを許可する手段とを備えることを特徴としている。このようにすれば、時間的条件付きアクセス許可を厳密に行うことが可能となる。

【００２６】さらにまた、本発明は、データファイルに格納されているデータに関連するポリシー記述を格納したリソースドキュメントと、外部からこのデータファイルにアクセスするためのアクセス要求を受け付けて、リソースドキュメントからこのアクセス要求のアクセス対象であるデータに関連付けられたポリシー記述を取り出して評価することにより、このアクセス要求を許可するか否かを決定するポリシー評価手段と、取り出されたポリシー記述中に、ポリシー評価手段が持つ情報だけでは評価できない条件がある場合に、他の処理を行うことによりこの条件の評価または実現が可能かどうかを判断する執行機能検証手段とを備えることを特徴としている。ここで、ポリシー評価手段が持つ情報だけでは評価できない条件を評価または実現するために必要な処理としては、アクセス対象であるデータファイルのデータ形式の変換や、アクセス対象であるデータファイルに対するアクセス履歴を残すといった動作がある。すなわち、これらの動作を実行することができる場合にのみ、ポリシー記述にこれらの条件を持つアクセス要求が許可されることとなる。

【００２７】

【発明の実施の形態】以下、添付図面に示す実施の形態に基づいてこの発明を詳細に説明する。まず、本発明の概要を説明すると、本発明では、アクセス制御において行うポリシー評価の結果を、従来のようなＹｅｓまたはＮｏの２値ではなく、ブール代数による多値とし、その

中間値を「この条件を満たせばＹｅｓ」と解釈する。これによって、ポリシー評価とそれを実現するための条件部の執行とを統一的に表現できる枠組みを提供する。この実現法としては、アクセス制御のためのポリシー記述をIf-then型ルールに拡張し、その評価に論理型言語の評価法である部分評価を用いる。そして、If部を、条件チェックと、実施のインストラクションの両方に用いる。これによって、ポリシーの記述が簡潔かつ宣言的になり、かつ、ポリシー全体の整合性が、論理型言語の枠組みで判断できるようになる。

【００２８】図１は、本実施の形態におけるアクセス制御システムを搭載するデータ管理サーバの構成を説明するための図である。同図において、符号２００はデータ管理サーバである。符号２１０はデータファイルであり、アクセス対象となるデータや文書を格納している。符号２２０はデータ管理サブシステムであり、データや文書を管理し、検索等のサービスを提供する。符号２３０はユーザ認証サブシステムであり、登録されたユーザだけがデータ管理サーバ２００の機能を利用できることを保証する。符号２４０はアクセス制御サブシステムであり、ユーザ認証サブシステム２３０と共に、特定のユーザによる特定のアクセス要求だけを受け付けて、データ管理サブシステム２２０が提供するサービスを利用できるようにアクセス制御する。また、データ管理サーバ２００は、アクセス制御サブシステム２４０によるアクセス制御に用いるために、管理されているデータや文書及びユーザに関連する各種の情報を外部から入力する。図示の例では、所定の外部ファイル３００からユーザのＩＤを補足するための当該ユーザが所属する組織の組織図を入力したり、タイムスタンプサーバ４００から時間情報を取得したりすることができる。

【００２９】データ管理サーバ２００に格納されている所望のデータや文書にアクセスしようとするユーザは、まず、ユーザ端末５００からデータ管理サーバ２００のユーザ認証サブシステム２３０にアクセスしてシステムにログインする。この際、ユーザ認証サブシステム２３０は、パスワードの照合等の手段により、当該ユーザが登録されているユーザ（管理されているデータや文書にアクセスが許されているユーザ）かどうかを判断する。次に、ユーザは、所望するデータへのアクセス要求をアクセス制御サブシステム２４０に対して発行する。アクセス制御サブシステム２４０は、ユーザ認証サブシステム２３０から受け取ったログイン情報や当該アクセス要求の内容、アクセス制御のためのセキュリティーポリシー等に基づいてアクセスの可否を判定する。この際、必要に応じて、組織図や時間情報等を入力してアクセス可否の判定に利用する。アクセス制御サブシステム２４０によるアクセス可否の判定の結果、アクセスが許可された場合は、データ管理サブシステム２２０によってデータファイル２１０から該当するデータまたは文書が読み出され、アクセス制御サブシステム２４０を介してユーザ端末５００へ送信される。詳細な動作については後述するが、アクセス制御サブシステム２４０は、ポリシー記述の内容によっては、読み出されたデータを変換したり、元のデータに履歴情報（ログファイル等）を追加したりすることができる。

【００３０】図２は、本実施の形態におけるアクセス制御システムの全体構成を説明するための図である。なお、図２のアクセス制御システム１００は、図１のアクセス制御サブシステム２４０に相当する。同図において、符号１０はポリシー評価モジュールであり、アクセス要求を受けて、アクセス対象であるデータに関連付けられたポリシー記述を評価する。符号２０は執行機能検証モジュールであり、ポリシー評価モジュール１０が持つ情報だけでは評価できない条件(以下、外部条件と呼ぶ)が評価対象のポリシー記述中にある場合に、当該外部条件の評価や実現が可能かどうかを判断する。符号３０は執行モジュールであり、執行機能検証モジュール２０により評価や実現が可能であると判断された外部条件の評価や実現を実行する。執行モジュール３０は、執行する外部条件の評価や実現の内容に応じて複数設けることができる。したがって、執行機能検証モジュール２０は、執行モジュール３０が複数ある場合には、ポリシー評価モジュール１０から受け取った外部条件の評価や実現が、用意されているいずれの執行モジュール３０により可能かについても検証する。符号４０はリソースドキュメントであり、アクセス対象であるデータに関連するポリシー記述を格納している。なお、アクセス制御システム１００はコンピュータにて実現され、上記各モジュールは当該コンピュータに上記各処理を実行させるためのプログラムモジュールとして実現される。

【００３１】図３は、図２中に示された、各モジュール１０、２０、３０に入出力されるデータの内容を定義するテーブルである。図３を参照すると、ポリシー評価モジュール１０に入力されるアクセス要求１１０、１３０の構成は（Subject, Object,Role (or Uid), Operation）であり、ポリシー評価モジュール１０から執行機能検証モジュール２０へ送られる外部条件の情報１１３の構成は条件リスト〔Condition-List〕であり、執行機能検証モジュール２０から執行モジュール３０へ送られる執行指示１２１の構成は執行を指示するデータセット〔Instruction-Set〕である。また、ポリシー評価モジュール１０によりリソースドキュメント４０から読み出されるポリシー記述１４０と、図１のデータファイル２１０からデータ管理サブシステム２２０を介して執行モジュール３０へ送られる文書１３４と、執行モジュール３０からデータ管理サブシステム２２０を介してデータファイル２１０へ送られる更新情報１３３とはＸＭＬ文書（XML Document）である。また、ポリシー評価モジュール１０、執行機能検証モジュール２０及び執行モジュ

ール３０からそれぞれ出力されるアクセス不許可１１２、１２０、１３１はアクセス要求に対する不許可を示すデータ列（a string of "denied"）であり、ポリシー評価モジュール１０から出力されるアクセス許可１１１はアクセス要求に対する許可を示すデータ列（a string of "permission"）であり、執行モジュール３０から出力されるリソーストランスコード１３２はＨＴＭＬ、ＸＭＬ等の文書やデータ列等（HTML, XML, string, etc.）である。

【００３２】図４は、図２に示した本実施の形態におけるアクセス制御システム１００がアクセス要求を処理する際の動作を説明するフローチャートである。図４に示される一連の処理は、ユーザーからのアクセス要求１１０により起動されるか、またはアクセス要求に対する処理の中で特定の執行モジュール３０により二次的に発行されるアクセス要求１３０により再帰的に起動される。アクセス要求１１０，１３０を受け付けると、ポリシー評価モジュール１０は、まず、アクセス対象である文書に対応するポリシー記述１４０をリソースドキュメント４０から検出し（ステップ４０１）、そのポリシー記述１４０を評価する（ステップ４０２）。そして、全てのポリシー記述１４０の中の条件が評価可能であれば、その評価結果に応じてアクセス許可１１１またはアクセス不許可１１２という結果を、当該アクセス要求１１０を発行したユーザに回答する（ステップ４０３、４０４、４０５）。

【００３３】これに対し、ポリシー記述１４０の中にポリシー評価モジュール１０だけでは評価できない条件があった場合は、条件付き許可と判定され、ポリシー評価モジュール１０から執行機能検証モジュール２０へ外部条件の情報１１３が渡される（ステップ４０３）。執行機能検証モジュール２０は、システム内に用意されている執行モジュール３０のリストを持っている。そこで、執行機能検証モジュール２０は、外部条件の情報１１３を受け取ると、当該外部条件を評価しまたは実現できる執行モジュール３０を検索する（ステップ４０６）。そして、適当な執行モジュール３０が見つからなかった場合、アクセス不許可１２０という結果を当該アクセス要求１１０を発行したユーザに回答する（ステップ４０７、４０８）。

【００３４】一方、当該外部条件を評価しまたは実現できる執行モジュール３０が見つかった場合は、該当する執行モジュール３０が呼び出されて当該外部条件の評価及び実現が行われる（ステップ４０７、４０９）。執行モジュール３０における当該外部条件の評価の結果がアクセス許可である場合、または条件の実現に成功した場合は、リソーストランスコード１３２が出されると共に、ポリシー評価モジュール１０に戻って、さらに他のポリシー記述１４０の評価が続行される（ステップ４１０）。そして、最終的にポリシー記述１４０の中の全ての条件が評価され、アクセス許可と判断されたならば、執行モジュール３０において出されたリソーストランスコード１３２と共にアクセス許可１１１という結果を当該アクセス要求１１０を発行したユーザに回答する。また、執行モジュール３０における当該外部条件の評価の結果がアクセス不許可である場合、または執行モジュール３０が当該外部条件の実現に失敗した場合は、アクセス不許可１３１という結果を当該アクセス要求１１０を発行したユーザに回答する（ステップ４１１）。

【００３５】ここで、執行モジュール３０での処理において、当該外部条件を満たすために他の文書やアクセス対象である文書中の他のセクションに対してアクセスが必要な場合は、アクセス要求１３０をポリシー評価モジュール１０に発行して、再帰的に評価させることができる。このように、外部条件を満たすために行われる再帰的なアクセス要求自体をアクセス許可の評価対象とすることにより、他段階の評価を行うことができ、セキュリティーを高めることができる。さらに、執行モジュール３０において、当該外部条件を満たすために当該ユーザが所属する組織の構成やアクセス日時といった個別の情報を必要とする場合は、それらの情報を提供するファイルやサーバにアクセスして必要な情報を取得することができる。

【００３６】次に、個々のモジュールに関して、機能を詳細に説明する。図５は、ポリシー評価モジュール１０によるポリシーの評価アルゴリズムを説明するフローチャートである。図６及び図７は、ポリシー評価モジュール１０に入出力されるデータのフォーマット及び表現例を説明する図である。図５を参照すると、まず、アクセス要求１１０を入力してパラメータを受け取る（ステップ５０１）。アクセス要求の書式は、図６のアクセス要求の欄を参照すると、アクセスを要求する主体（ユーザなど）を識別するデータである Subject と、アクセス対象を識別するデータである Object と、アクセス対象に対する操作を識別するデータである Operation とをパラメータとする。このパラメータは、「SubjectがObjectに対してOperationの操作権限(アクセス権)を要求している」を意味する。また、図６には、アクセス要求の具体例が記載されており、SubjectがNihon Taroh/IBM/Japanであり、Objectがhttp://admin.trl.com//form/expense.xmlであり、Operationがread(html)であるようなアクセス要求がなされたことを示している。このアクセス要求は「Nihon Taroh/IBM/Japanというユーザ名でログインしたユーザが、admin.trl.comサーバに置かれているexpense.xmlというファイルに対して、ＨＴＭＬ形式での読み取りを要求する」ことを意味している。なお、ここでは入力をアクセス要求１１０としたが、執行モジュール３０から出力されたアクセス要求１３０を入力した場合も同様の処理を行う。

【００３７】次に、リソースドキュメント４０の中に格

納されているアクセス制御用のポリシー記述の中から、アクセス要求パラメータの全てのパラメータ（Subject, Object, Operation）と合致する規則を検索する（ステップ５０２）。そして、検出したポリシー規則１４０を入力として受け取る。ポリシー規則の書式は、図６のアクセス制御ポリシー規則の欄を参照すると、アクセス許可ユーザを識別するデータである Subject と、アクセス許可対象を識別するデータである Object と、アクセス許可操作を識別するデータ Operation と、アクセスを許可する条件の記述である Condition とをパラメータとする。このパラメータは、「Conditionの条件が満足された時、SubjectがObjectに対してOperationの操作権限を持つ」というルールを意味する。また、図６にはポリシー規則の具体例が記載されており、Subjectがemployeeであり、Objectがhttp://admin.trl.com//form/expense.xmlであり、Operationがread(html)であり、Conditionがtranscode(in, out)であるようなポリシー規則を示している。このポリシー規則は「employeeというロール（データにアクセスするための資格）をもったユーザまたはアプリケーションに対して、データをＨＴＭＬに変換することができる場合に限り、admin.trl.comサーバに置かれているexpense.xmlというファイルに対して読み取りを行うことを許可する」ということを意味している。

【００３８】ここで、合致とは、Subject、Object、Operation等の値がそれぞれ整合することである。例えば、アクセス評価要求パラメータのSubjectが‘amano’ならば、アクセス制御ポリシー規則の中で‘amano’というユーザＩＤや‘amano’を含むＴＲＬというグループ名が記述されている規則が合致して取り出される。

【００３９】また、アクセス制御ポリシー規則の検索において、パラメータとの合致の検証に用いるために、リソースドキュメント４０の中に格納されている環境データも受け取る。環境データの書式は、図７の環境データの欄を参照すると、ポリシー評価モジュール内で真である事実の列挙や任意の事実である Environment をパラメータとする。このパラメータは、「Environmentはポリシー評価時に真として扱う」を意味する。また、図７には、環境データの具体例が記載されており、Nihon Taroh/IBM/Japanというユーザはemployeeというロールになることができるという事実が環境データとして存在することを示している。この環境データを図６のアクセス要求及びポリシー規則の具体例に適用すれば、アクセス要求にあるNihon Taroh/IBM/Japanというユーザがポリシー規則のemployeeというロールをもったユーザという条件を満たすことがわかる。

【００４０】次に、規則検証処理として、ステップ５０２で合致したポリシー規則が複数ある場合に、どのように複数のポリシー規則を評価するかを決定する（ステップ５０３）。例えば、ポリシー規則に優先度が指定されている場合はその優先度順に正しく評価されるように並べ替えたり、アクセス不許可をアクセス許可より優先させるというルールを用意してポリシー規則を二つに分類し並べ替えるなどの処理を行う。このようにすれば、不用意にアクセスを許可してしまうことを防止することができる。合致した規則がない場合の処理もここで規定する。例えば、閉世界ポリシーの場合は無条件にアクセス不許可とする。

【００４１】次に、ステップ５０３で処理されたポリシー規則の条件部を評価する（ステップ５０４）。ポリシー規則の条件部にリソースドキュメント４０に存在する値を使った条件が記述されている場合、当該リソースドキュメント４０から該当する値を取り出す。当該条件部の中で、リソースドキュメント４０から取り出された値に基づいた条件は評価可能であるとする。

【００４２】次に、ステップ５０３の評価結果を判定し（ステップ５０５）、全ての条件が評価可能でありかつ全てが真と評価される場合はアクセス許可とする（ステップ５０６）。また、全ての条件が評価可能でありかつ一つ以上の条件が偽となる場合はアクセス不許可とする（ステップ５０８）。さらにまた、評価不可能な条件がある場合は、当該評価できない条件だけからなる外部条件を作成し、条件付きアクセス許可の条件として、執行機能検証モジュール２０へ処理を移行する（ステップ５０７）。外部条件の書式は、図７の外部条件の欄を参照すると、ポリシー評価モジュール１０内で真であるかどうか不明の事実のリストである ExternalCondition をパラメータとする。このパラメータは、「アクセス制御ポリシー規則のConditionの中で、環境データや、ポリシー評価モジュールのシステム関数などを使って即時に真偽を判断できない条件」を意味する。また、図７には外部条件の具体例が記載されており、図６のアクセス要求及びポリシー規則を評価した結果、ポリシー評価モジュール１０から執行機能検証モジュール２０へ、expense.xmlをＨＴＭＬに変換することができるかどうかを意味する外部条件が送信されることを意味する。執行機能検証モジュール２０の処理へ移行した後は、執行モジュール３０による処理を経て再びポリシー評価モジュール１０に処理が戻り、最終的な評価結果の判定がなされる。ただし、後述するように、執行機能検証モジュール２０または執行モジュール３０において当該外部条件を評価できないまたは実現できないと判断された場合は、ポリシー評価モジュール１０に戻ることなくアクセス不許可となる。

【００４３】図８は、執行機能検証モジュール２０による執行機能検証アルゴリズムを説明するフローチャートである。図９は、執行機能検証モジュール２０が用いるデータのフォーマットを説明する図である。図８を参照すると、まず、ポリシー評価モジュール１０から送られた条件付きアクセス許可における外部条件の情報を入力

すると共に、執行機能検証モジュール２０に内蔵されている執行モジュールリストから、執行モジュール３０として登録されているComponentの情報を読み出す（ステップ８０１）。執行モジュールリストから受け取る執行モジュール３０に関する情報の書式は、図９を参照すると、条件付きアクセス要求の条件部である Condition Expression と、条件を処理できるコンポーネントの有無を示す Capability と、条件を処理するコンポーネントを示す Component Name と、コンポーネントの引数である Component Argument とをパラメータとする。図９には執行モジュール３０に関する情報の具体例が記載されており、Condition Expressionがtranscode#type#1(*.xml, html)であり、Capability CheckがAvailableであり、Component Nameがc:¥tools¥jar¥enforcerl.jarであり、Component Argumentがc:¥enforcement¥transcode#type#1.xslであるような情報が存在することを示す。この情報は「transcode#type#1という外部条件を満たすEnforcement機構が利用可能であり、enforcerl.jarというプログラムにtranscode#type#1.xslというパラメータファイルを与えてデータを処理することにより条件の実現が可能である」ということを意味している。

【００４４】次に、外部条件として入力した複数の条件から順番に一つずつ条件を取り出す（ステップ８０２）。そして、ステップ８０１で取得したCondition Expressionの中に、ステップ８０２で取り出された条件を満たすエントリーがあるかどうかをチェックする（ステップ８０３）。そのようなエントリーがある場合は、更に次の条件とCondition Expressionとの照合を行い、外部条件を構成する全ての条件に対して照合が終わるまで処理を繰り返す（ステップ８０４）。一方、外部条件を構成する条件のうち一つでも、その条件を満たすエントリーがなかった場合は、アクセス不許可１２０を出力して処理を終了する（ステップ８０５）。

【００４５】以上のようにして、外部条件を構成する全ての条件に関してその条件を満たすエントリーが検出されたならば、すなわち、外部条件におけるパラメータが全て検証されたならば、執行モジュール３０による処理へ移行する。このときの執行モジュール３０への執行指示１２１の書式は、執行モジュールリストから読み出された情報におけるComponent NameとComponent Argumentの組み合わせを複数のリストとして構成したものである。例えば、((lotusxsl.jar, transcode.xsl) (domhash.jar, signature.xml))である。

【００４６】図１０は、執行モジュール３０の構成例を説明する図である。図１０を参照すると、執行モジュール３０は、書き込み／変更対象検出手段３１と、ＸＳＬプロセッサ３２と、プラグイン可能なフィルタプログラム３３とを備える。書き込み／変更対象検出手段３１は、ＸＭＬ文書における書き込みや変換を行う部分を検出する。ＸＳＬプロセッサ３２は、ＸＭＬデータと変換ルールを読み込んで新たなＸＭＬデータを生成する標準のツールである。フィルタプログラム３３は、ＸＳＬプロセッサ３２では処理できない内容の執行指示を実現するプログラムであり、プラグインにより所望の機能を用意することができる。執行モジュール３０による執行処理は、データファイル２１０の中のＸＭＬ文書に対してある種の変換操作を施し、別のＸＭＬ文書を生成する処理として実現される。執行処理の具体的な内容をしめす執行指示１２１は、ＸＭＬ文書に対する変換ルールを記述したＸＳＬデータとして表現される。

【００４７】図１１は、執行モジュール３０による執行処理を説明するフローチャートである。図１１を参照すると、まず、書き込み／変更対象検出手段３１は、ＸＳＬで記述された変換ルール（執行指示１２１）を解析し、変換対象であるＸＭＬ文書１３４に対して書き込みや変更が行われる可能性がある部分を検出する（ステップ１１０１）。ここで、執行モジュール３０による処理は、最初のアクセス要求１１０に対する評価に必要な条件を満足するために実行される処理であることから、変換対象であるＸＭＬ文書は、必ずしもアクセス要求１１０のアクセス対象であるとは限らない。例えば、アクセス要求１１０のアクセス対象であるデータファイルに関連する他のファイルである場合もある。また、検出は、例えば対象文書１３４に試験的に変換ルールを適用してみて元の文書との木構造を比較することにより行う。執行処理に伴い、元データの書き込みや変更の必要があることがわかった場合には、ポリシー評価モジュール１０へアクセス要求１３０を行って問い合わせる（ステップ１１０２）。そして、ポリシー評価モジュール１０がアクセスを許可された場合にのみ当該処理を続行する（ステップ１１０３）。

【００４８】ポリシー評価モジュール１０によりアクセスが不許可とされた場合は、それまでに行った執行命令の処理を元にもどし、あるいは一時データに対して行った処理をリソースドキュメント４０に書き戻さずに（ステップ１１０８）、条件の実現に失敗したことを執行機能検証モジュール２０及びポリシー評価モジュール１０に通知して終了する（ステップ１１０９）。これにより、当該条件の評価または実現が不可能であり、当該条件を含むアクセス要求が不許可１３１となる。

【００４９】ポリシー評価モジュール１０によりアクセスが許可された場合は、ＸＳＬプロセッサ３２が、変換対象であるＸＭＬ文書１３４の変換を行う（ステップ１１０４）。暗号化や透かし等のように、執行としての詳細な手続きを、ＸＳＬで直接記述できない場合は、ＸＳＬプロセッサ３２によって暗号化や透かしのための指示のみを対象ＸＭＬ文書１３４に挿入しておく。そして、実際の処理は、適当なフィルタプログラム３３によって行う（ステップ１１０５）。

【００５０】執行指示１２１に記述された全ての変換処

理が終了した時点で、執行モジュール３０は、執行機能検証モジュール２０及びポリシー評価モジュール１０に条件が実現されたことを通知して終了する（ステップ１１０６、１１０７）。ＸＳＬプロセッサ３２とフィルタプログラム３３によって生成された執行済みＸＭＬ文書データは、更新情報１３３として、データ管理サブシステム２２０を介してデータファイル２１０に書き戻されるか、またはリソーストランスコード１３２としてアクセス許可の回答１１１と共にアクセス要求１１０の発行元に対して開示される。

【００５１】次に、本実施の形態を用いた具体的な実施例について説明する。まず、本実施の形態を用いてデータのトランスコーディングを行う実施例について説明する。ここで、トランスコーディングとは、単一のソースで記述された情報をアクセス要求者のセキュリティーレベルや通信路、表示デバイスの性能等に応じてフォーマットを変換して通信することをいう。ここでは、ＸＭＬベースで記述された帳票情報（各フィールドの意味を示す名前がXMLのタグで記述されている）に読み取り要求が発行されたとき、再利用可能性の度合いの低いＨＴＭＬ形式ならば読み取りを許可する、といったポリシー記述がある場合の実施例を示す。このポリシー規則は例えば次のように記述される。acl(*, role(employee), doc(http:// trl.ibm.com/xmlform/X), read(Form)) <- transcode(X, xml, Form).

【００５２】これに対し、旅費申請フォームをＨＴＭＬ経由で読みたいというアクセス要求が発行されたものとする。このアクセス要求は例えば次のように記述される。

?-acl(amano, role(employee) doc(http://trl.ibm.com/xmlform/ travelExpenseAccount.xml) ,read(html)).

この場合、Subjectがポリシー記述、アクセス要求共にrole(employee)で一致し、アクセス要求のObjectがdoc(http://trl.ibm.com/xmlform/ travelExpenseAccount.xml)で、ポリシー記述のObjectであるdoc(http:// trl.ibm.com/xmlform/X)に含まれるものの、Operationであるread(html)に対してtranscode(X, xml,Form)というConditionが付けられているので、ポリシー評価モジュール１０による評価の結果は条件付アクセス許可となる。ポリシー評価モジュール１０から執行機能検証モジュール２０へ送られる外部条件は、ＸＭＬフォームをＨＴＭＬに変換できればアクセスを許可するという条件であり、例えば次のように記述される。

transcode(travelExpenseAccount.xml, xml, html)

【００５３】したがって、アクセス制御システム１００がＸＭＬで記述された対象フォームをＨＴＭＬに変換する執行モジュール３０を持っていれば、アクセスが許可されることとなる。かかる執行モジュール３０がある場合、執行モジュール３０には、ＸＭＬで記述された対象フォームをＨＴＭＬに変換するためのＸＳＬ記述が与えられる。ＸＳＬプロセッサ３２は、このＸＳＬ記述と元のフォームデータを処理して表示用のＨＴＭＬデータを生成する。そして、生成されたＨＴＭＬデータが当該アクセス要求を発行したユーザへ返送される。

【００５４】次に、本実施の形態を用いて文書に電子透かしを挿入する実施例について説明する。かかる処理は、トランスコーディングの変形例として扱うことができる。すなわち、ポリシー記述としてＸという画像中に，アクセスしたユーザのＩＤを埋め込むならばアクセスを許可するという条件を用意しておく。この条件を含む規則は、例えば図値のように記述される。

acl(user(ID), role(subscriber), doc(http:// trl.ibm.com/image/X), read)<- embed(X, ID).

電子透かしのように処理が複雑で執行の詳細な手続きを直接記述できない場合は、ＸＳＬプロセッサ３２においては、電子透かしを埋め込むのための指示のみを対象文書に挿入するようにする。そして、実際に電子透かしを埋め込む処理は、専用のフィルタプログラム３３によって行う。データファイルを暗号化するならばアクセスを許可するといった条件を与える場合等の執行命令も同様の方法で実現することができる。

【００５５】次に、本実施の形態を用いてデータへのオペレーションに関してログ（log）ファイルへの書き込みを行う実施例について説明する。アクセス制御を行うシステムにおいて、オーディタビリティ（耐監査性）を確保することは重要である。そのためには、特定のデータへのオペレーションに関してログ(履歴)を残す仕組みがあると便利である。ここでは、どういう場合にログを取らなくてはいけないかをポリシーとして記述しておき、執行する実施例を示す。このポリシー記述は例えば次のように記述される。

acl(user(ID), role(issuer), doc(http:// trl.ibm.com/xmlform/X), write(*)) <- status(log(ID, issuer, X, write, T)).

【００５６】これに対し、次のようなアクセス要求が発行されたものとする。

?-acl(amano, role(issuer) doc(http://trl.ibm.com/xmlform/ travelExpenseAccount.xml#linputfield) ,write("cost=$100")).

この場合、Subjectがポリシー記述、アクセス要求共にrole(issuer)で一致し、アクセス要求のObjectがdoc(http://trl.ibm.com/xmlform/ travelExpenseAccount.xml#linputfield)で、ポリシー記述のObjectであるdoc(http:// trl.ibm.com/xmlform/X)に含まれるものの、Operationであるwrite("cost=$100")に対してstatus(log(ID, issuer, X, write, T)というConditionが付けられている。ここで、statusが以下のようなルールであるものとする。

status(log(Subj, Role, Obj, Op, T)) <- log(Subj, Role, Op, T).

status(log(Subj, Role, Obj, Op, T)) <- makelog(Subj, Role, Op, T).
この場合、まだlogという状態データは書きこまれていないので，statusの第１のルールは失敗する。そして、第２のルールが適用されて、makelog(..)が条件となる条件付アクセス許可となる。

【００５７】makelogの要求を受けた執行モジュール３０は、対応する執行指示１２１を解析して元データへの書き込みが必要であることを検出する。そして、書き込み許可を得るために、ポリシー評価モジュール１０に対してログ書き込みのためのアクセス要求１３０を出す。このアクセス要求１３０は、例えば次のように記述される。

?-acl(sys1, role(system) doc(http://trl.ibm.com/xmlform/ travelExpenseAccount.xml#log) ,write(log(amano, issuer, travelExpenseAccount.xml#issuerField, write("cost=$100"))).

これのアクセス要求１３０は、再度ポリシー規則を評価することによって可否が判断される。ここで、アクセスが許されたとすると、ログの書き込みが行われ、更に元のアクセス要求についても、条件が満たされることによってアクセスが許されることとなる。したがって、最終的に、元のアクセス要求に関して、そのログがアクセス対象である文書中に保存されることになる。

【００５８】実際のログへの書き込み処理は、トランスコーディングの場合と同様にＸＭＬ文書間の変換ルールとして記述される。例えば、パーツのオーダー情報に関するアクセスのログを残すために図１２のような記述（ＸＳＬの変換ルールの書き方に従っている）を用意してシステムに登録しておく。これは"GR Head"という部品に関する数量と納期に関する情報を誰に開示したかということを記録するための記述である。図１２中の楕円で囲んだ&Subject;の部分は、執行処理の実行時に指定されるパラメータ（この場合はアクセス要求の発行元）である。そして、&Subject;の部分を実際の会社名等に置き換えた記述とオーダー情報を記述した執行処理対象文書をＸＳＬプロセッサ３２で処理することにより、図１３に示すようなログが追加された文書が生成される。

【００５９】次に、本実施の形態を用いて時間条件付きアクセス許可を行う実施例について説明する。インターネット上で入札や競売を行う場合、「この情報は何月何日の何時以降ならば読んでも良い」というような条件を付けたアクセス制御を厳密に行う必要がある。ここでは、何時以降にアクセス可能になるかというポリシーの記述について説明する。そのようなポリシーは、時間条件付きアクセス許可(Temporal Authorization)と呼ばれる。従来そのようなアクセス許可のポリシー記述は、次のように表現される。

acl(AnyUserID, role(employee), doc(http://announce/bonus.xml), read) :-get#time(T), T > "1999/06/03".

これは、「employeeロールを持つユーザは、http://announce/bonus.xmlを、１９９９年６月３日以後ならばread権限を持つ」という意味である。この場合、get#timeというシステム述語が現在時刻を求め、１９９９年６月３日よりも後ならば条件が満たされ、employeeはbonus.xmlに対してread権限を持つことができる。

【００６０】このようなアクセス許可を実行した場合、アクセス制御のセキュリティーがサーバのシステムクロックの値に依存してしまうという問題点がある。例えば、システム管理者がアクセス制御を行うサーバのシステムクロックを故意に変更した場合、本来はread権限がない時間にemployeeがreadできてしまう。readアクセスをログに残したとしても、アクセス時刻の値にシステムクロックを使うと仮定すると、時限アクセス許可に対する不正アクセスを検知することができない。また、サーバのシステムクロックに対しては、ＯＳレベルでのアクセス制御が行われていると仮定する場合が多い。しかし、以上のアクセス許可では、時間条件付きアクセスについてＯＳレベルの仮定は必要ない。

【００６１】これに対し、本実施の形態を時間条件付きアクセス許可に用いた実施例では、アクセス許可のポリシー記述は、次のように表現される。

acl(user(ID), role(employee), doc(http://announce/bonus.xml), read) :- status(timestamp(S,T)), verify#signature(S), T > "1999/06/03".

これに対し、アクセス制御システム１００は、各モジュールごとに、以下のように処理を行う。

【００６２】まず、ポリシー評価モジュール１０において、当該ポリシー記述の評価を行う。ここで、status(timestamp(S,T))に関して次のルールが記述されているとする。

status(timestamp(S,T)) :- timestamp(S,T).
status(timestamp(S,T)) :- get#timestamp(S,T), makelog(timestamp(S,T)).

timestamp(S,T)というタイムスタンプデータは、まだリソースドキュメント４０に書き込まれていないので、statusの第１のルールは失敗する。そして、第２のルールが適用され、get#timestamp(S,T), makelog(timestamp(S,T))が条件となる条件付きアクセス許可となる。verify#signature(S)とT > "1999/06/03"は、ポリシー評価モジュール１０では評価できないので、同様にして条件付きアクセス許可となる。最終的に、get#timestamp(S,T)、 makelog(timestamp(S,T))、verify#signature(S)、及びT > "1999/06/03"が外部条件１１３となって、ポリシー評価モジュール１０から執行機能検証モジュール２０へ送られる。

【００６３】次に、執行機能検証モジュール２０において、当該外部条件を評価または実現できる執行モジュール３０の有無を検証する。ここで、執行機能検証モジュ

ール２０は、図１４に示すようなテーブルを持っているものとする。図１４に示すテーブルは、Condition Expressionで表現された内容を処理できる執行モジュール３０の有無、及び処理できる執行モジュール３０のComponent名を定義したものである。図１４のテーブルにおいて、makelog/1は、１引数のmakelog述語を意味する。formula#expressionとは、四則演算などを含む式表現を意味する。これから、条件付きアクセス許可の全ての条件部が執行モジュール３０を用いて処理できることがわかる。そこで、執行機能検証モジュール２０から執行モジュール３０へ、〔timestamp#processor,get#timestamp(S,T)〕、〔log#processor,makelog(timestamp(S,T))〕、〔siganture#processor, verify#signature(S)〕、及び〔formula#processor,T > "1999/06/03"〕)が執行指示１２１として送られる。

【００６４】次に、執行モジュール３０において、各執行指示１２１に応じた処理を行う。以下、個別に説明する。

get#timestamp(S,T)に対する処理

get#timestampは、タイムスタンプ・プロセッサにより処理を行う。タイムスタンプ・プロセッサには、次のような執行処理プログラムが記述されている。get#timestamp(S,T) :- get#trust(timestamp, C), get#timestamp(C,T,S).ここで、get#trust/2は、データファイル２１０からtrustの記述を取り出す述語である。例えば元の文書に次のようなtrust記述がある場合を考える。

trust(timestamp, "http://www.surety.com").

これは、文書がtimestampとして"surety"を信用することを意味する。データファイル２１０から文書１４１を検索した結果として、get#trustの変数Cには、"http://www.surety.com"が割り当てられる。この後、get#timestamp述語により、Surety Timestamp Serviceから時刻Tのタイムスタンプ Sが得られる。これで、執行指示１２１の最初の条件は満足した。尚、本実施例において、Timestamp ServiceはSuretyに限定することを意味しない。元の文書が信用するどのようなサービスも記述可能である。

【００６５】makelog(timestamp(S,T))に対する処理

makelogは、ログ・プロセッサにより処理を行う。ログ・プロセッサは、以下のようなログの書込みのためのアクセス要求１３０を発行する。

acl(sys1, role(system), doc(http://announce/bonus.xml#log), write)

そして、再度ポリシー規則を評価することによってログの書き込みの可否が判断される。アクセス制御システム１００がログに書き込みを行う権限を持つ場合、執行モジュール３０に対して、ポリシー評価モジュール１０からアクセス許可がなされる。これにより、makelogはlog(timestamp(signature#value, 1999/06/04))のタイムスタンプの書込みを行う。

【００６６】verify#signature(S)に対する処理

verify#signatureは、署名プロセッサにより処理を行う。タイムスタンプの署名値を検証し、Validなら真（正しい署名）、Invalidなら偽（誤った署名）を返す。なお、Suretyの署名値はValidだと仮定する。

【００６７】T > "1999/06/03"に対する処理

式表現は、書式プロセッサにより処理を行う。Tはタイムスタンプの時刻の値、すなわち1999/06/04である。これは、T > "1999/06/03"なので処理結果として真（正しい書式）を返す。

【００６８】以上により、執行機能検証モジュール２０から執行モジュール３０へ送られた、get#timestamp(S,T)、makelog(timestamp(S,T))、verify#signature(S)、及びT > "1999/06/03"の各執行指示１２１は全て真となる。これにより、結果的にポリシー評価モジュール１０において要求された、acl(user(ID), role(employee), doc(http://announce/bonus.xml), read)の条件は全て満たされたこととなる。

【００６９】ここで、最初に説明した時間条件アクセス許可の問題が解決されていることを説明する。上記の例でアクセスが許可された場合、元の文書のログ領域には必ずタイムスタンプの値が追加されている。タイムスタンプの値は所定の時刻に生成されたことを意味するが、そのタイムスタンプの値がログ領域にあるということは、タイムスタンプ時刻よりも現在時刻は必ず後であることを意味する。従って、仮にシステム管理者がポリシー評価モジュール１０や執行モジュール３０のシステムクロックの値を変更していたとしても、タイムスタンプの値を参照することによって時間条件を正しく検証できることを意味する。

【００７０】

【発明の効果】以上説明したように、本発明によれば、アクセス制御において、アクセス要求に対してアクセスを許すか許さないかを判断するだけでなく、ある条件を満たせばアクセスを許すという条件付きのアクセス許可を評価することができる。また、条件付きのアクセス許可において評価される条件が更に他の条件を満足することを要求する場合に、再帰的に当該他の条件に対する評価も行うことができる。

【図面の簡単な説明】

【図１】　本実施の形態におけるアクセス制御システムを搭載するデータ管理サーバの構成を説明するための図である。

【図２】　本実施の形態におけるアクセス制御システムの全体構成を説明するための図である。

【図３】　アクセス制御システムの各モジュールに入出力されるデータの内容を定義するテーブルである。

【図４】　アクセス制御システムがアクセス要求を処理する際の動作を説明するフローチャートである。

【図５】　ポリシー評価モジュール１０によるポリシー

の評価アルゴリズムを説明するフローチャートである。

【図６】　ポリシー評価モジュール１０に入出力されるデータのうち、アクセス要求とポリシー規則のフォーマット及び表現例を説明する図である。

【図７】　ポリシー評価モジュール１０に入出力されるデータのうち、環境データと外部条件のフォーマット及び表現例を説明する図である。

【図８】　執行機能検証モジュール２０による執行機能検証アルゴリズムを説明するフローチャートである。

【図９】　執行機能検証モジュール２０が用いるデータのフォーマットを説明する図である。

【図１０】　執行モジュール３０の構成例を説明する図である。

【図１１】　執行モジュール３０による執行処理を説明するフローチャートである。

【図１２】　データへのオペレーションに関してログファイルへの書き込みを行う実施例において、文書にアクセスのログを残すための記述を説明する図である。

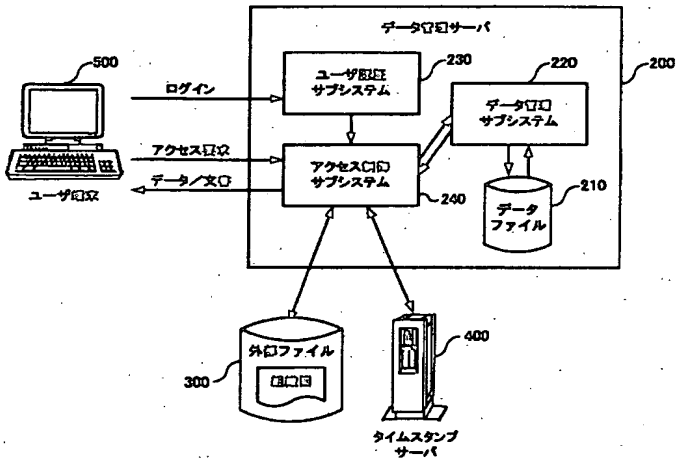
【図１３】　図１２の記述に応じて文書にログが追加された状態を説明する図である。

【図１４】　執行機能検証モジュール２０が執行モジュールの検証を行うために用いるテーブルを例示して説明する図である。

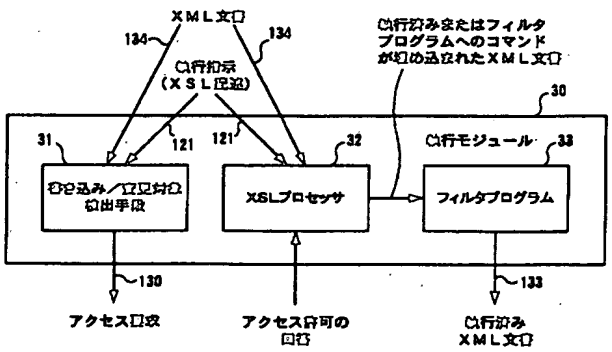
【符号の説明】

１０…ポリシー評価モジュール、２０…執行機能検証モジュール、３０…執行モジュール、４０…リソースドキュメント、１００…アクセス制御システム、２００…データ管理サーバ、２１０…データファイル、２２０…データ管理サブシステム、２３０…ユーザ認証サブシステム、２４０…アクセス制御サブシステム

【図１】



【図１０】

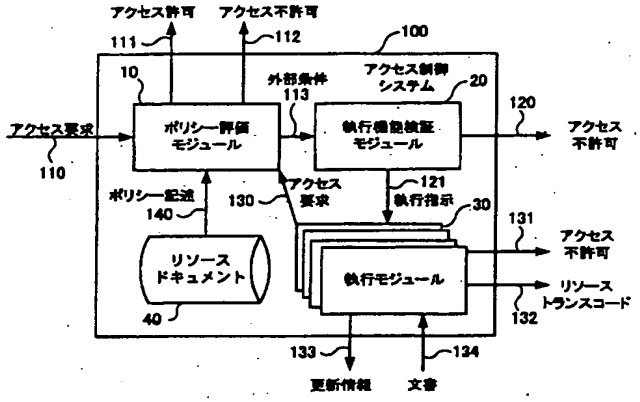


【図１２】

XSLによるEmforcement記述の例

```
<xsl:t□□ate □tch="/">
 <xsl:copy>
  <xsl:apply-t□□lates select="@|O|□□nt()|el()|text()"/>
 </xsl:copy>
 <Log disclosedto="ASubject:">
 <xsl:for-each select="Order[Parts[□□='□□ Head']]">
  Parts □□ :□□ Head
  Quantity  :<xsl:value-of select="Quantity"/>
  Delivery Dau:<xsl:value-of select="DeliveryDate"/>
 </xsl:for-each>
 </Log>
</xsl:t□□ate>
</xsl:stylesheet>
```

【図２】

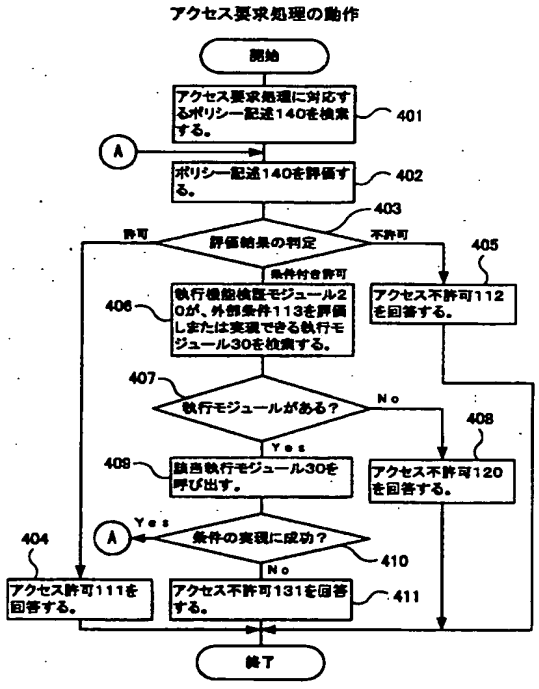


【図３】

各モジュールの入出力データ

Data Type	Components
Access Request	(Subject, Object, Role (or Uid), Operation)
External Condition	[Condition-List]
Enforcement Instruction	[Instruction-Set]
Resource Retrieval	XML Document
Policy Retrieval	XML Document (rule syntax)
Resource Update	XML Document
Access Deny	a string of "denied"
Resource Transcode	HTML, XML, string, etc.

【図４】



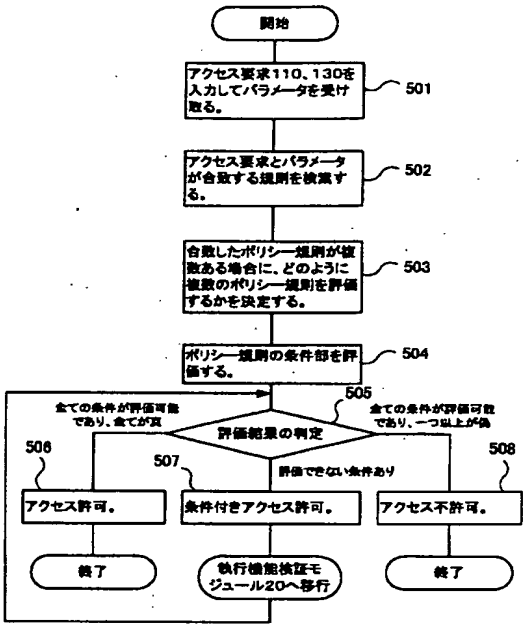
【図１４】

実行モジュールのテーブル

Condition Expression	Capability	Component Name
mkslog/1	○	log_processor
get_timestamp/2	○	timestamp_processor
verify_signature/1	○	signature_processor
formula_expression	○	formula_processor

【図５】

ポリシー評価モジュールの動作



【図６】

ポリシー評価モジュール10に入出力されるデータのフォーマット及び表現例

入出力	データフォーマット
アクセス要求	● パラメータ: Subject: アクセスを要求する主体(ユーザなど)を識別するデータ。ユーザID、ロール名など。 Object: アクセス対象を識別するデータ。データエレメント名など。 Operation: アクセス対象に対する操作を識別するデータ。読み込み、書き込みなど。 ● 意味: Subject が Object に対して Operation の操作権限を持つかどうかアクセス要求する。 ● 具体例: Subject: Nihon Taroh/IBM/Japan Object: http://admin.trl.com//form/expense.xml Operation: read(html) ● Prologによるアクセス要求の表現例: query(user(Nihon Taroh/IBM/Japan),_ 'http://admin.trl.com//form/expense.xml', read(html)).
アクセス制御ポリシー規則	● パラメータ: Subject: アクセス許可ユーザを識別するデータ。 Object: アクセス対象を識別するデータ。 Operation: アクセス許可操作を識別するデータ。 Condition: アクセスを許可する条件の記述。 ● 意味: Condition の条件が満足されたとき、Subject が Object に対して Operation の操作権限を持つというルール。 ● 具体例: Subject: employee Object: http://admin.trl.com//form/expense.xml Operation: read(html) Condition: transcode(in, out) ● Prologによるアクセス要求の表現例: act(_role(employee),'http://admin.trl.com//form/expense.xml', read(Format)) :- transcode(Nihon Taroh.xml, Format).

【図７】

ポリシー評価モジュール10に入出力されるデータのフォーマット及び表現例

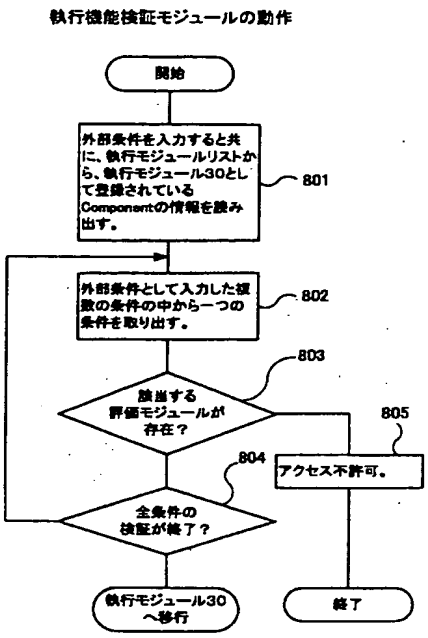
入出力	データフォーマット
環境データ	● パラメータ: Environment: ポリシー評価モジュール内で真である事実の列挙。任意の事実。 ● 意味: Environment はポリシー評価時に真として扱う。 ● 具体例: Nihon Taroh/IBM/Japan というユーザは employee というロールになることができるという事実。 ● Prologによるアクセス要求の表現例: Environment(role(Nihon Taroh/IBM/Japan, employee)).
外部条件	● パラメータ: ExternalCondition: ポリシー評価モジュール内で真であるかどうか不明の事実リスト。 ● 意味: ExternalCondition は、アクセス制御ポリシー規則のCondition の中で、現場データや、ポリシー評価モジュールのシステム時刻などを使って即時に真偽を判断できない条件を意味する。 ● 具体例: expense.xml を html に変換することができるかどうかを意味する外部条件 ● Prologによるアクセス要求の表現例: transcode(expense.xml, html).

【図９】

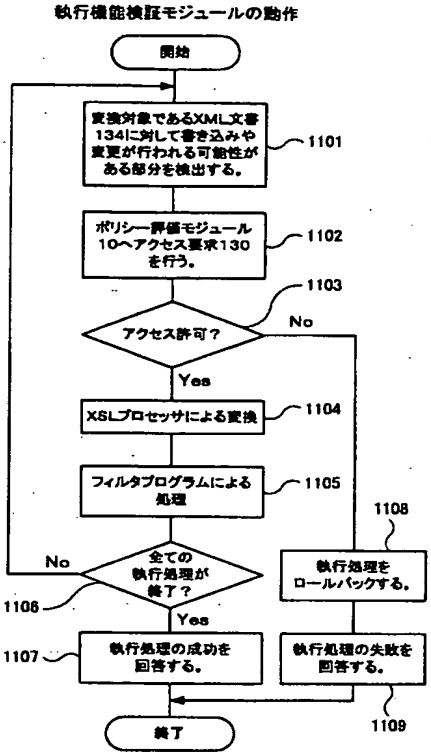
執行機能検証モジュール20が用いるデータのフォーマット

入出力	データフォーマット
Capability Repository (執行モジュール30に関する情報)	● パラメータ: Condition Expression: 条件付きアクセス要求の条件部。 Capability: 条件を処理できるコンポーネントの有無。 Component Name: 条件を処理するコンポーネント。 Component Argument: コンポーネントの引数。 ● 意味: Condition Expression は、条件を処理するときに、アクセス制御ポリシーの中に記述される条件の表現形式である。 Capability は Capability Check コンポーネントにおいて有効か無効かをオンするフラグ。 Component Name は、条件を処理するプログラムコンポーネント、URLなどで記述する。 Component Argument は、コンポーネントが使う引数。 Condition Expression の引数や、URLなどで記述する。 ● 具体例: Condition Expression: transcode_type_1(e.xml, html) Capability Check: Available Component Name: c:¥tools¥jar¥enforcer.jar Component Argument: c:¥enforcement¥transcode_type_1.sal

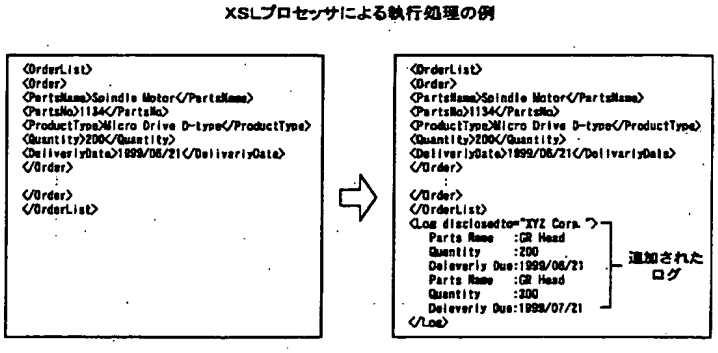
【図８】


実行機能検証モジュールの動作
開始
外部条件を入力すると共に、実行モジュールリストから、実行モジュール30として登録されているComponentの情報を読み出す。
801
外部条件として入力した複数の条件の中から一つの条件を取り出す。
802
803
該当する評価モジュールが存在？
805
アクセス不許可。
804
全条件の検証が終了？
実行モジュール30へ移行
終了

【図１１】


実行機能検証モジュールの動作
開始
変換対象であるXML文書134に対して書き込みや変更が行われる可能性がある部分を検出する。
1101
ポリシー評価モジュール10へアクセス要求130を行う。
1102
1103
アクセス許可？
No
Yes
XSLプロセッサによる変換
1104
フィルタプログラムによる処理
1105
1108
No
全ての実行処理が終了？
1106
実行処理をロールバックする。
Yes
1107
実行処理の成功を回答する。
実行処理の失敗を回答する。
終了
1109

【図１３】


XSLプロセッサによる実行処理の例
<OrderList>
<Order>
<PartsName>Spindle Motor</PartsName>
<PartsNo>1134</PartsNo>
<ProductType>Micro Drive D-type</ProductType>
<Quantity>200</Quantity>
<DeliveryDate>1999/06/21</DeliveryDate>
</Order>
:
</Order>
</OrderList>
<OrderList>
<Order>
<PartsName>Spindle Motor</PartsName>
<PartsNo>1134</PartsNo>
<ProductType>Micro Drive D-type</ProductType>
<Quantity>200</Quantity>
<DeliveryDate>1999/06/21</DeliveryDate>
</Order>
:
</Order>
</OrderList>
<Log disclosedto="XYZ Corp.">
Parts Name :CR Head
Quantity :200
Delevery Due:1999/06/21
Parts Name :CR Head
Quantity :200
Delevery Due:1999/07/21
</Log>
追加されたログ

フロントページの続き

(72)発明者　沼尾　雅之
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内
(72)発明者　工藤　道治
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内
(72)発明者　天野　富夫
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

Ｆターム(参考)　5B017 AA01 BA05 BA07 BB02 BB10 CA16
5B082 AA11 EA10 EA11 EA12 GA14 GC04